Global Privacy Best Practices

BSA는 글로벌 소프트웨어 산업을 대변하는 선도적 옹호자로서, 클라우드 컴퓨팅, 데이터 분석 및 인공 지능을 비롯한 최첨단 혁신 기술의 개발에 앞장서고 있습니다. 소프트웨어 사용 기술은 기능을 수행하기 위해 점점 더 많은 데이터(경우에 따라 개인 데이터)를 사용하게 됩니다. 결과적으로, 개인 데이터 보호는 BSA 회원사에 중요한 우선순위입니다. 따라서 BSA는 개인 데이터 보호가 고객 신뢰 구축의 핵심 요소임을 인식하고 있습니다. 개인 데이터 보호의 목적을 달성하기 위해 BSA는 개인정보보호에 대한 사용자 중심 접근법을 권장합니다. 이 접근법은 소비자에게 해당 개인 데이터를 제어할 수 있는 메커니즘을 제공합니다. 또한 BSA는 개인 데이터의 사용이 소비자의 기대에 부합하도록 하는 동시에 기업이 합법적인 비즈니스 이익을 추구할 수 있도록 하는 데이터 보호 프레임워크를 지원합니다.

전 세계 국가가 데이터 보호 프레임워크 개발을 고려할 때 많은 국가가 이러한 문제에 접근하기 위한 글로벌 모범 사례를 파악하려고 했습니다. BSA는 개인 데이터 수집 및 사용의 투명성을 제고하고, 이러한 수집 및 사용에 대한 거버넌스를 제공함으로써 정보에 근거한 선택을 가능하게 하고 이를 존중하며, 소비자에게 개인 데이터에 대한 제어권을 제공하고, 강력한 보안을 제공하며, 합법적인 비즈니스 목적을 위한 데이터 사용을 촉진하는 모범 사례의 구현을 지원합니다. BSA는 이러한 목표를 달성하는 데 도움이 되며 전 세계의 데이터 보호 프레임워크를 개발 및 수정하는 데 유용한 지침 역할을 할 수 있는 아래의 모범 사례를 강조합니다.

문제	모범 사례
특정 지역 범위	데이터 보호 프레임워크는 국가와 충분히 긴밀하게 연관된 행동을 관리해야 합니다. 법률은 다음의 경우에 적용되어야 합니다. (1) 거주자를 명확하게 대상으로 지정한 경우 (2) 처리 대상인 개인 데이터를 수집 당시에 해당 국가의 데이터 주체로부터 의도적으로 수집한 경우 그리고 (3) 현실적이고 효과적인 수준의 활동을 야기하는 안정된 약정을 통해 해당 국가에 설립된 법인에서 그러한 수집을 수행한 경우
개인 데이터의 정의	개인 데이터의 정의 안에 포함되는 정보의 범위는 확인된 소비자 또는 확인 가능한 소비자와 관련된 정보여야 합니다. 확인 가능한 소비자란 소비자의 이름, 식별 번호, 위치 데이터, 온라인 식별자 또는 소비자의 신체적, 생리적 또는 유전적 정체성과 관련된 하나 이상의 요인과 같은 식별자를 참조하여 합리적 노력을 통해 직접 또는 간접적으로 확인할 수 있는 소비자를 의미합니다. 다루는 정보의 범위는 잘못 취급될 경우 소비자의 개인정보보호에 유의미한 영향을 미치는 개인 데이터와 관련이 있어야 합니다. 재확인의 위험을 합리적으로 줄일 수 있는 강력한 기술 및 조직적 조치를 통해 식별 정보가 제거된 데이터는 프레임워크에서 다루는 데이터가 아닙니다.
피해	데이터 보호 프레임워크는 소비자에게 해를 끼칠 수 있는 위험에 맞춰 보호 조치를 조정해야 합니다. 신체 상해, 건강에 좋지 않은 영향, 재무적 손실 또는 소비자의 합리적 기대를 벗어나 구체적으로 부정적인 결과를 초래할 가능성이 상당히 있는 민감한 개인 데이터의 공개를 인지할 수 있는 피해로 고려해야 합니다.
투명성	데이터 컨트롤러는 수집하는 개인 데이터의 범주, 데이터를 공유할 제3자의 유형 및 컨트롤러가 개인 데이터를 검토, 변경 요청, 사본 요청 또는 삭제하기 위해 유지 관리하는 프로세스에 대한 설명을 비롯하여 개인 데이터를 취급하는 관행에 대한 명확하고 이해하기 쉬운 설명을 제공해야 합니다.

문제	모범 사례
목적의 명확성	개인 데이터는 합법적인 방법으로 수집 및 취득한 목적에 적절해야 합니다. 컨트롤러는 소비자에게 개인 데이터를 수집하는 목적을 알려야 하며, 해당 설명, 트랜잭션의 맥락 또는 소비자의 합리적인 기대와 일치하는 방식으로 또는 데이터를 수집한 원래 목적과 양립할 수 있는 방식으로 해당 데이터를 사용해야 합니다. 컨트롤러는 명시된 목적과 양립할 수 있는 방식으로 개인 데이터를 사용 및 공유하도록 보장하는 거버넌스 시스템을 사용해야 합니다.
데이터 품질	개인 데이터는 사용 시 목적에 적절해야 하며, 해당 목적에 필요한 정도까지 정확하고 완전하며 최신 상태여야 합니다.
처리의 근거	데이터 보호 프레임워크는 트랜잭션의 맥락 또는 소비자의 기대와 일치하는 합법적인 비즈니스 목적을 비롯하여 여러 타당한 이유로 데이터 처리를 인식하고 지원해야 합니다. 다른 타당한 목적에는 계약 수행과 관련된 처리, 공공의 이익이나 소비자의 중요한 이익을 위한 처리, 법적 의무 준수에 필요한 처리 또는 소비자의 동의에 따른 처리가 포함됩니다. 데이터 보호 프레임워크는 조직의 합법적인 사이버 보안 활동, 사기 또는 신원 도용을 탐지하거나 방지하려는 조치의 구현, 기밀 정보를 보호할 수 있는 능력, 법적 청구의 행사 또는 방어 등을 제한해서는 안 됩니다.
동의	컨트롤러는 소비자가 정보에 근거하여 선택할 수 있게 하며, 실질적이고 적절한 경우 개인 데이터 처리를 거부할 수 있는 기능을 제공해야 합니다. 동의가 적절한 환경에서, 동의는 트랜잭션의 맥락 또는 조직의 소비자와의 관계에 적절한 방식으로 한 번에 제공되어야 합니다.
민감한 개인 데이터 처리	금융 계좌 정보, 건강 상태 등의 특정 데이터는 특히 민감할 수 있습니다. 민감한 데이터 처리로 인해 개인정보보호 위험이 높아지는 경우 컨트롤러는 민감한 데이터의 수집 대상인 소비자가 확실한 명시적 동의를 선택할 수 있도록 해야 합니다.
소비자 제어	소비자는 조직이 자신과 관련된 개인 데이터를 보유하고 있는지 여부와 그러한 데이터의 특성에 관한 정보를 요청할 수 있어야 합니다. 소비자는 해당 데이터의 정확성에 대해 이의를 제기하고 적절한 경우 데이터를 수정 또는 삭제할 수 있어야 합니다 또한 소비자가 조직에 제공했거나 직접 생성한 개인 데이터의 복사본을 해당 소비자가 얻을 수 있어야 합니다. 조직은 소비자에게 이 정보를 제공하기 위한 적절한 수단 및 형식을 결정할 수 있는 유연성이 있어야 합니다. 개인 데이터 처리 수단 및 목적을 결정하는 컨트롤러는 이러한 요청에 응답할 주요 책임이 있습니다. 컨트롤러는 요청에 응답하는 데 따른 부담 또는 비용이 불합리하거나 소비자의 개인정보보호에 대한 위험과 균형이 맞지 않는 경우 또는 법적 요구 사항 준수, 네트워크 보안 보장, 그 밖의 기밀 상업 정보 보호를 위해서 또는 연구 목적으로 또는 언론의 자유나 다른 소비자의 다른 권리나 개인정보보호를 침해하지 않기 위해 그러한 요청을 거부할 수 있습니다. 또한 컨트롤러는 보안 검증 절차를 구현하여 부적절한 정보 공개의 피해 위험을 해결하도록 요청하는 소비자를 인증해야 합니다.

문제	모범 사례
보안 및 침해 알림	컨트롤러 및 프로세서는 개인 데이터에 대한 무단 액세스, 파괴, 사용, 수정 및 공개를 방지하도록 설계된 합리적이고 적절한(데이터의 양 및 민감도, 비즈니스의 규모 및 복잡성 그리고 사용 가능한 도구의 비용과 관련하여) 보안 조치를 채택해야 합니다. 데이터 컨트롤러는 신분 도용, 금융 사기 등의 중대한 위험을 초래하는, 암호화되지 않은 개인 데이터 또는 민감한 정보가 삭제되지 않은 개인 데이터의 무단 취득과 관련된 개인 데이터 침해를 알게 되면 가능한 한 빨리 소비자에게 알려야 합니다. 그러한 침해는 책임 요구 사항의 일부로, 조직이 취한 보안 조치와 함께 정기적으로 감독 당국에 보고될 수 있습니다.
책임 요구 사항	컨트롤러는 여기에 설명된 보호 조치를 제공하는 정책 및 절차를 개발해야 합니다. 여기에는 이러한 보호 조치를 시행하고 직원 교육 및 관리를 제공하여 프로그램을 조정할 담당자의 지정, 해당 프로그램의 실행에 대한 정기적인 모니터링 및 평가 그리고 필요한 경우 문제가 발생할 때 해당 문제를 해결하기 위한 방침 조정이 포함됩니다. 이러한 조치의 일환으로 컨트롤러는 민감한 데이터를 처리할 때 주기적으로 위험 평가를 수행할 수 있으며, 중요한 피해 위험을 파악한 경우 적절한 보호 조치의 시행을 문서화할 수 있습니다. 정부는 위험 평가를 보고하거나 규제 당국과 사전 협의하도록 하는 요구 사항을 부과해서는 안 됩니다. 이는 불필요한 관리 부담을 초래하고 개인정보 보호에 대한 상응하는 이점 없이 중요한 서비스 제공을 지연시키기 때문입니다.
국가 간 데이터 전송	데이터 보호 프레임워크는 세계 경제를 뒷받침하는 글로벌 데이터 흐름을 지원하고 장려해야 합니다. 전 세계적으로 데이터를 전송하는 조직은 국가 외부로 전송한 데이터가 계속 보호되도록 하는 절차를 구현해야 합니다. 데이터 보호 제도 간에 차이가 있는 경우 정부는 개인정보를 보호하는 동시에 글로벌 데이터 전송을 촉진하는 방식으로 해당 차이를 극복할 수 있는 도구를 만들어야 합니다. 데이터 보호 프레임워크는 공공 및 민간 부문 모두에 대해 데이터 현지화 요구 사항을 금지해야 합니다. 이는 보안 조치를 구현하려는 노력을 좌절시키고 비즈니스 혁신을 저해하며 소비자가 사용할 수 있는 서비스를 제한할 수 있습니다.
컨트롤러 및 프로세서 의무/책임 할당	개인 데이터 처리 수단 및 목적을 결정하는 데이터 컨트롤러는 법적 개인정보보호 및 보안 의무를 이행할 주요 책임이 있습니다. 컨트롤러를 대신하여 데이터를 처리하는 데이터 프로세서는 계약상 동의에 따라 컨트롤러의 지시를 따라야 할 책임이 있습니다. 컨트롤러 및 프로세서는 법에 의해 규정된 의무적인 규범적 표현 없이 고유한 계약 조건을 협상할 수 있는 유연성이 있어야 합니다.
구제 방법 및 처벌	중앙 규제 기관은 효과적인 집행을 보장하는 데 필요한 도구 및 리소스를 보유해야 합니다. 구제 방법 및 처벌은 데이터 보호법 위반으로 인한 피해에 비례해야 합니다. 민사 처벌은 독단적으로 부과해서는 안 되며 또는 근본적인 피해가 발생한 정황과 상당한 관련성이 없는 요인을 기반으로 해서는 안 됩니다. 형사상 처벌은 데이터 보호법 위반에 대해 비례적인 해결책이 아닙니다.